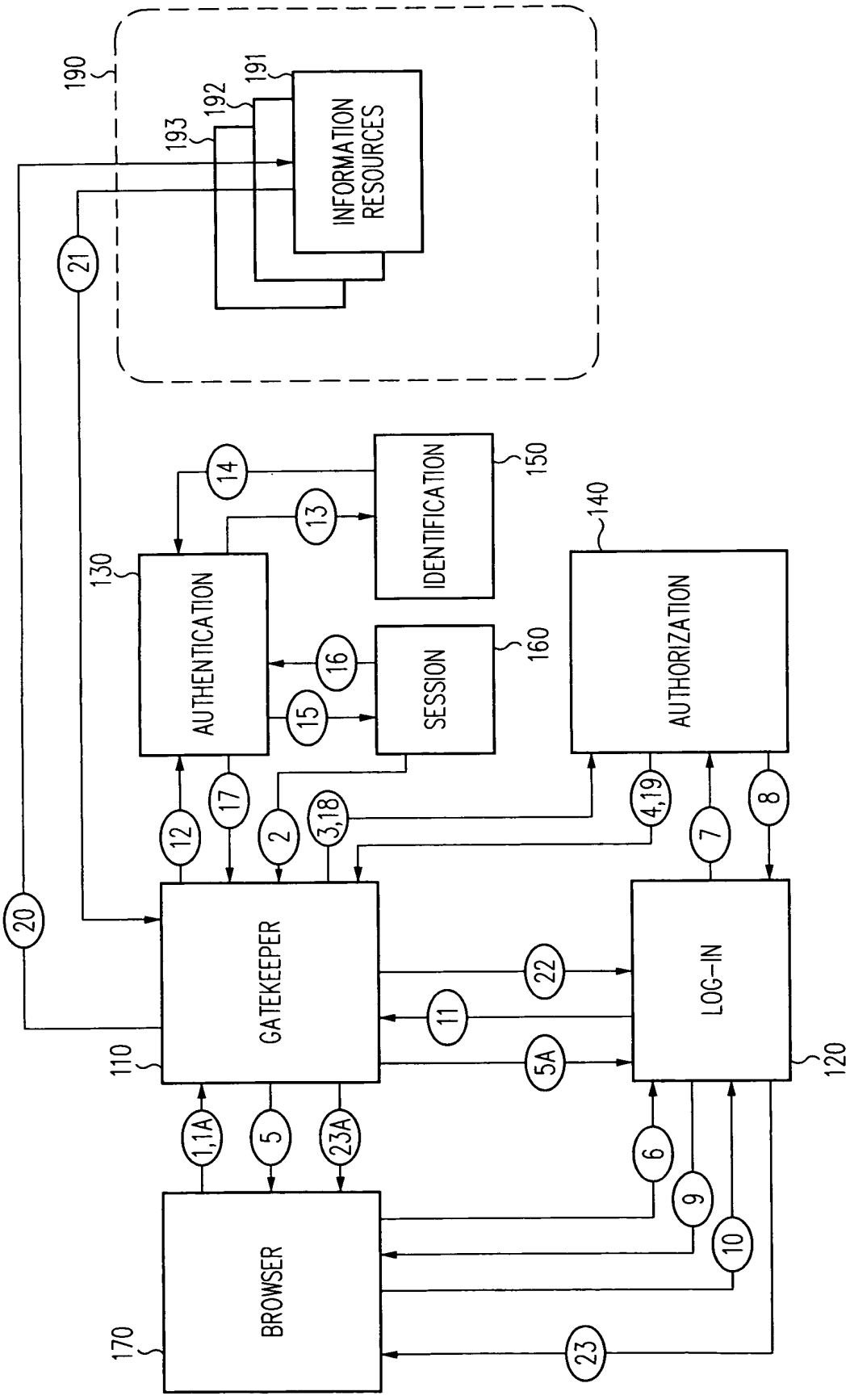
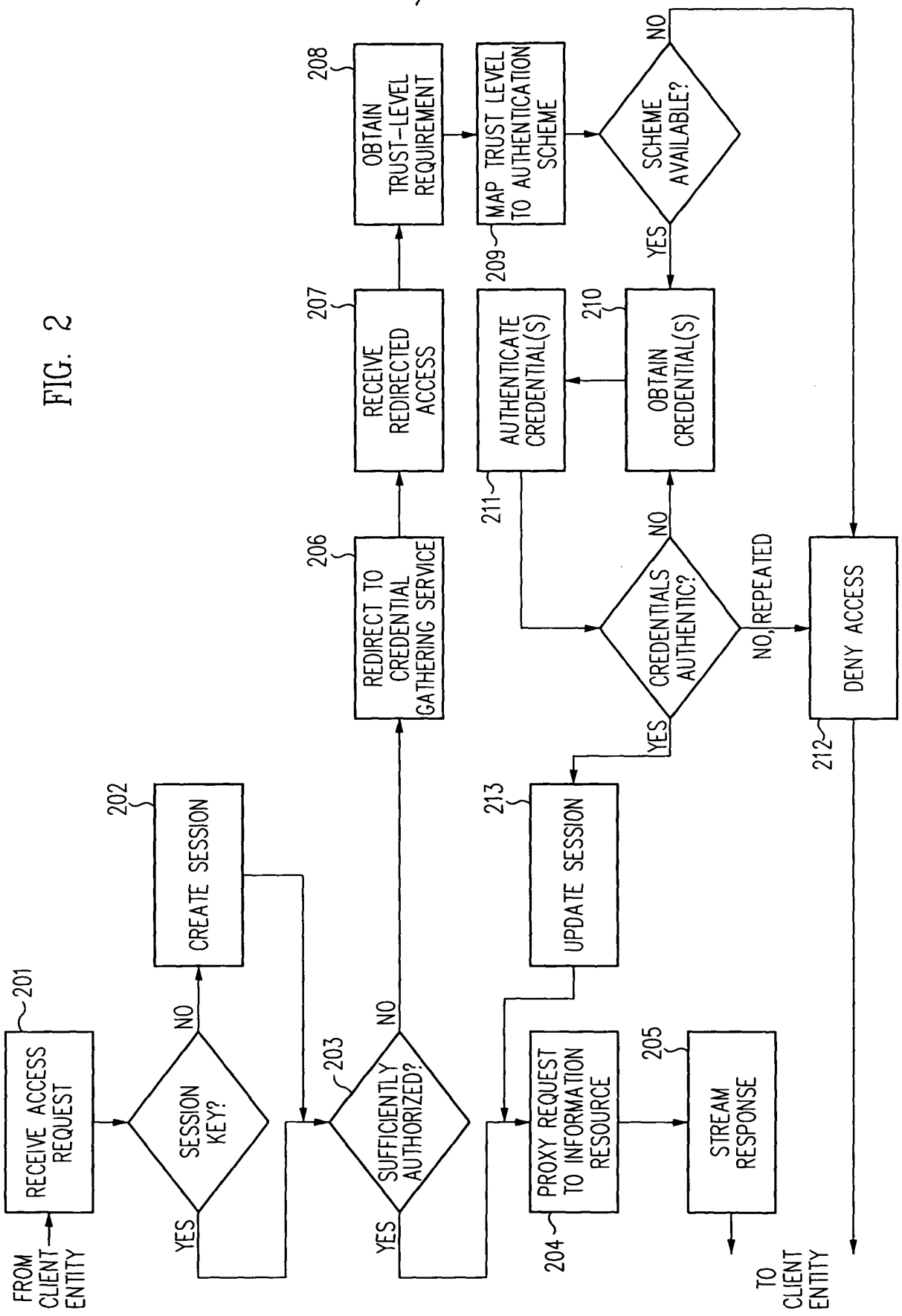
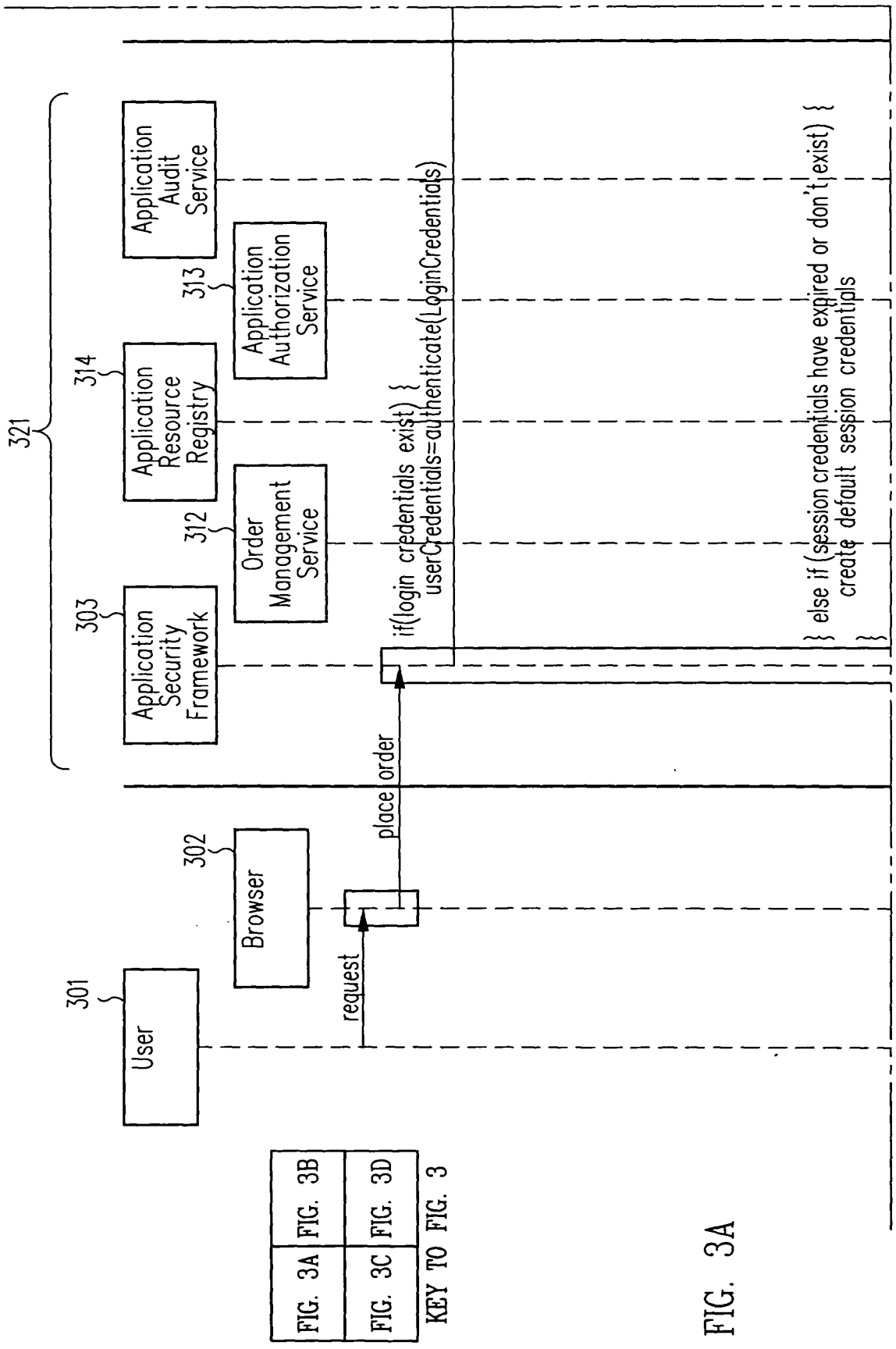

190
191
192
193
INFORMATION RESOURCES
21
14
13
IDENTIFICATION
150
140
130
AUTHENTICATION
16
15
SESSION
160
AUTHORIZATION
12
17
2
3,18
4,19
7
8
20
GATEKEEPER
22
11
5A
LOG-IN
110
120
1,1A
5
23A
6
9
10
BROWSER
170
23

FIG. 1

FIG. 2


FROM CLIENT ENTITY
RECEIVE ACCESS REQUEST
201
SESSION KEY?
NO
YES
CREATE SESSION
202
SUFFICIENTLY AUTHORIZED?
203
NO
YES
REDIRECT TO CREDENTIAL GATHERING SERVICE
206
RECEIVE REDIRECTED ACCESS
207
OBTAIN TRUST-LEVEL REQUIREMENT
208
MAP TRUST LEVEL TO AUTHENTICATION SCHEME
209
SCHEME AVAILABLE?
NO
YES
AUTHENTICATE CREDENTIAL(S)
211
OBTAIN CREDENTIAL(S)
210
CREDENTIALS AUTHENTIC?
NO
YES
NO, REPEATED
DENY ACCESS
212
UPDATE SESSION
213
PROXY REQUEST TO INFORMATION RESOURCE
204
STREAM RESPONSE
205
TO CLIENT ENTITY


321
301
User
302
Browser
303
Application Security Framework
312
Order Management Service
314
Application Resource Registry
313
Application Authorization Service
Application Audit Service
request
place order
if(login credentials exist) {
userCredentials=authenticate(LoginCredentials)
} else if (session credentials have expired or don't exist) {
create default session credentials
}
FIG. 3A
FIG. 3B
FIG. 3C
FIG. 3D
KEY TO FIG. 3

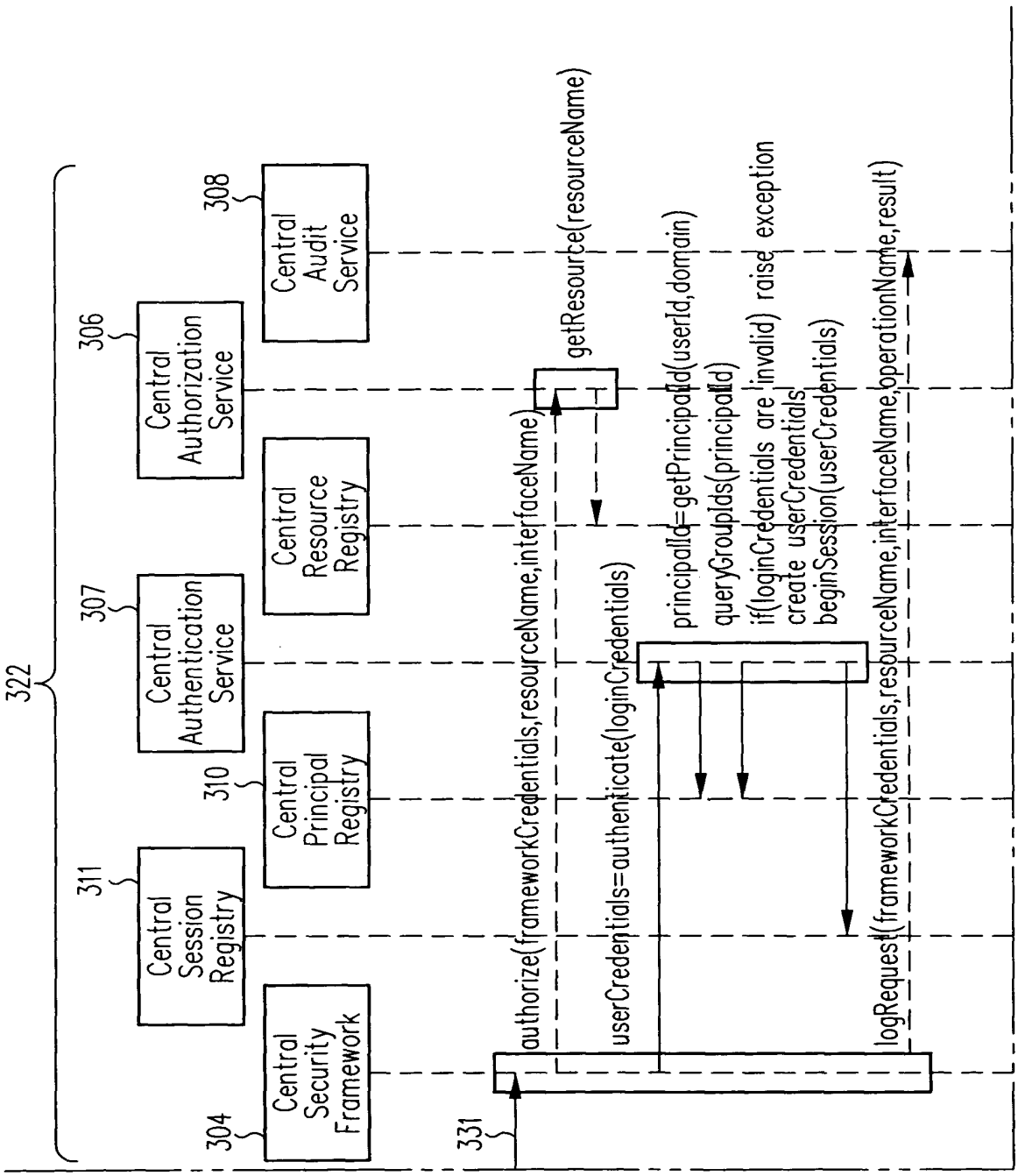

322
304
Central Security Framework
311
Central Session Registry
310
Central Principal Registry
307
Central Authentication Service
Central Resource Registry
306
Central Authorization Service
308
Central Audit Service
331
authorize(frameworkCredentials,resourceName,interfaceName)
getResource(resourceName)
userCredentials=authenticate(loginCredentials)
principalId=getPrincipalId(userId,domain)
queryGroupIds(principalId)
if(loginCredentials are invalid) raise exception
create userCredentials
beginSession(userCredentials)
logRequest(frameworkCredentials,resourceName,interfaceName,operationName,result)

FIG. 3B

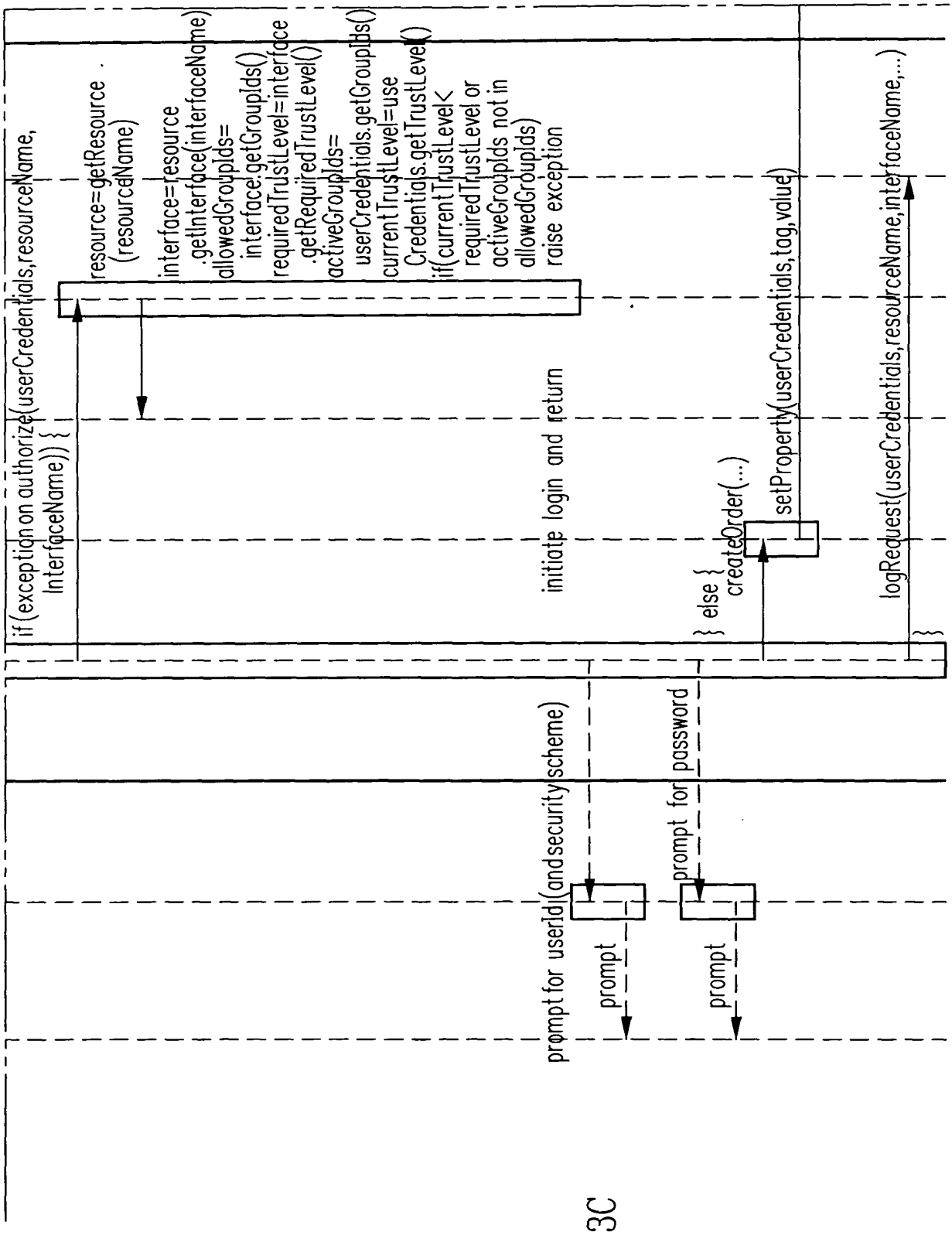
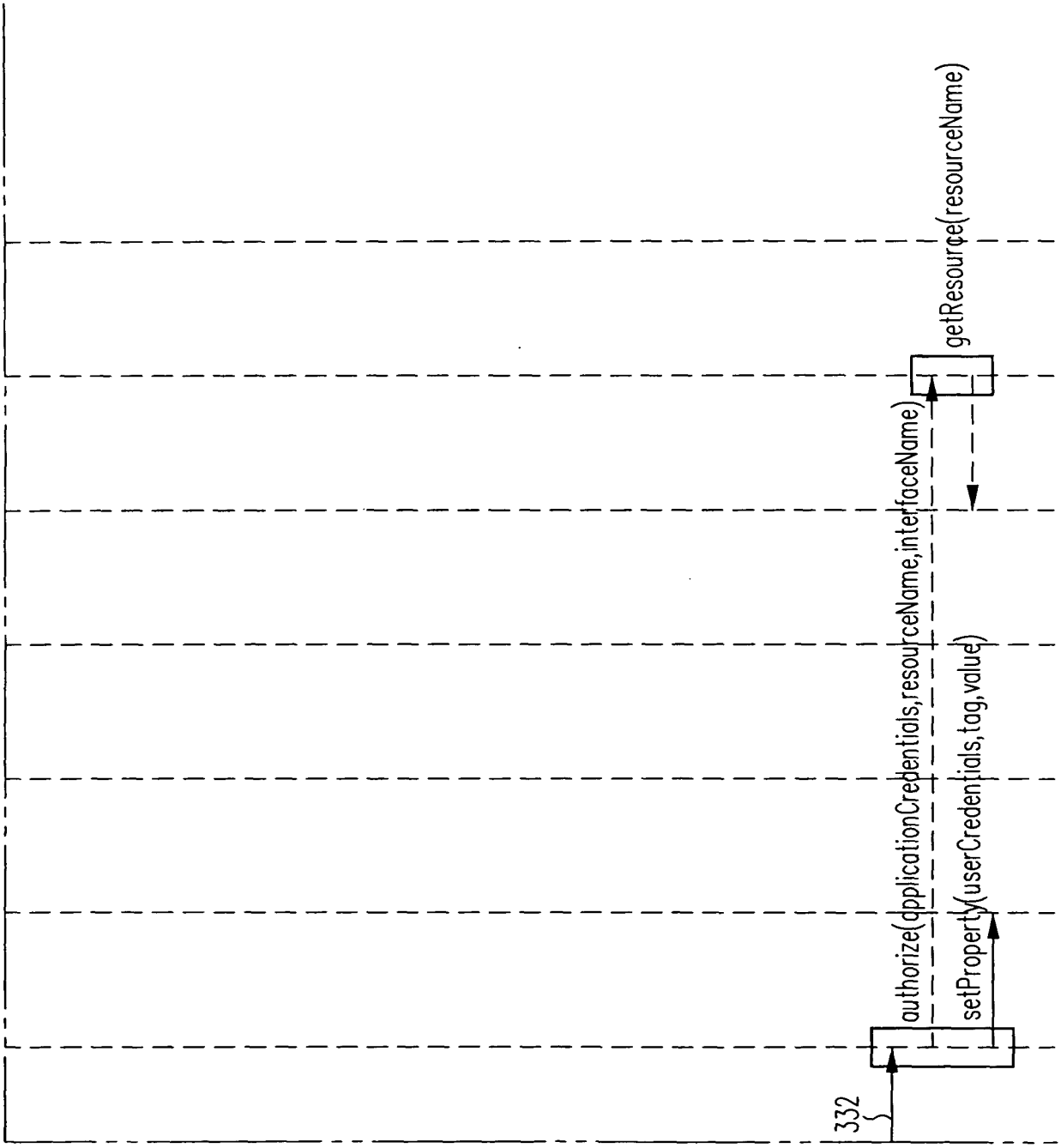

if (exception on authorize(userCredentials,resourceName,
InterfaceName)) {
resource=getResource
(resourceName)
interface=resource
.getInterface(interfaceName)
allowedGroupIds=
interface.getGroupIds()
requiredTrustLevel=interface
.getRequiredTrustLevel()
activeGroupIds=
userCredentials.getGroupIds()
currentTrustLevel=use
Credentials.getTrustLevel()
if(currentTrustLevel<
requiredTrustLevel or
activeGroupIds not in
allowedGroupIds)
raise exception
initiate login and return
} else {
createOrder(...)
setProperty(userCredentials,tag,value)
logRequest(userCredentials,resourceName,interfaceName,...)
prompt for userId(and security scheme)
prompt
prompt for password
prompt

FIG. 3C

FIG. 3D


getResource(resourceName)
authorize(applicationCredentials,resourceName,interfaceName)
setProperty(userCredentials,tag,value)
332

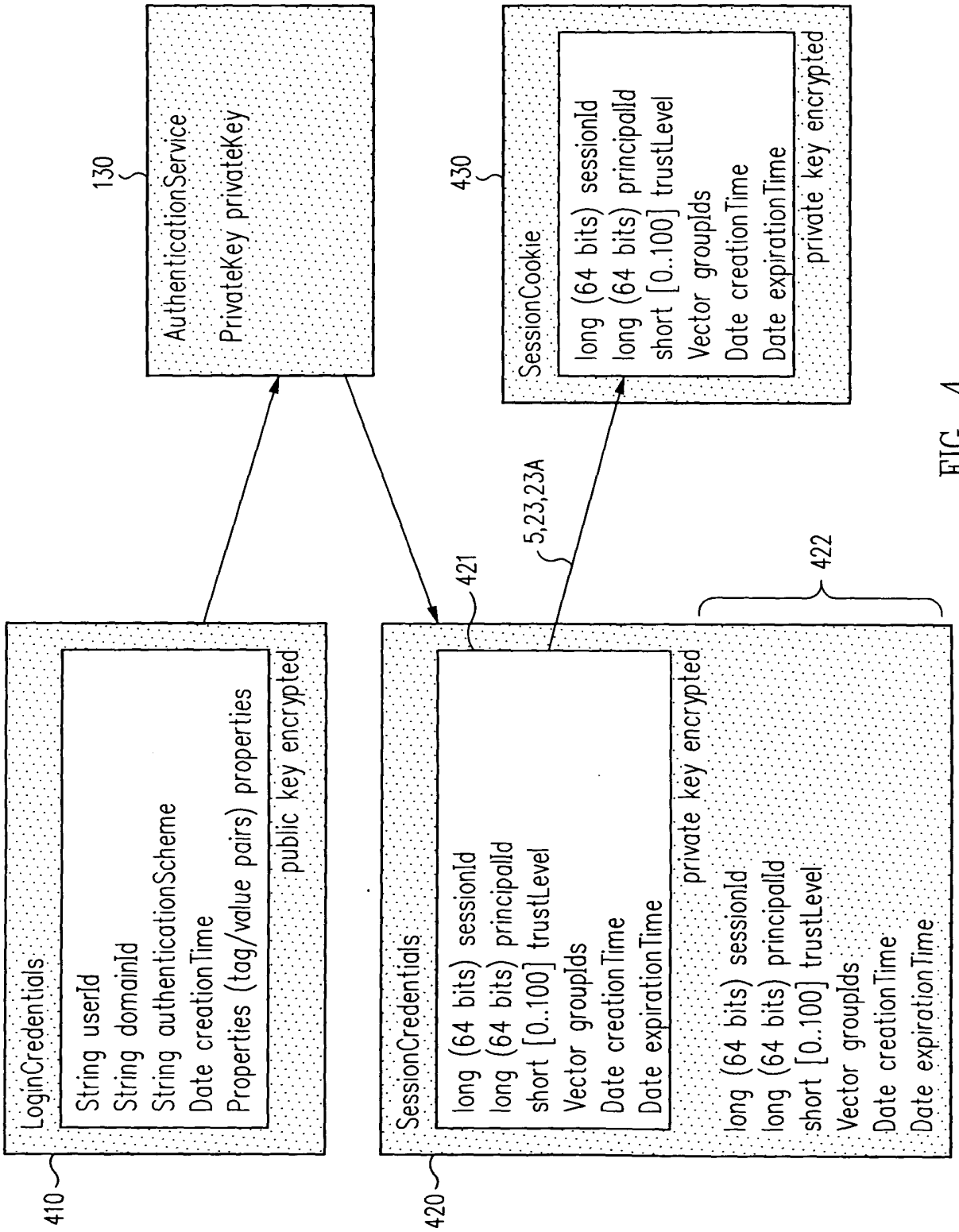

130
AuthenticationService
PrivateKey privateKey
430
SessionCookie
long (64 bits) sessionId
long (64 bits) principalId
short [0..100] trustLevel
Vector groupIds
Date creationTime
Date expirationTime
private key encrypted
5,23,23A
421
422
LoginCredentials
String userId
String domainId
String authenticationScheme
Date creationTime
Properties (tag/value pairs) properties
public key encrypted
SessionCredentials
long (64 bits) sessionId
long (64 bits) principalId
short [0..100] trustLevel
Vector groupIds
Date creationTime
Date expirationTime
private key encrypted
long (64 bits) sessionId
long (64 bits) principalId
short [0..100] trustLevel
Vector groupIds
Date creationTime
Date expirationTime
410
420

FIG. 4